IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Y. YOKOMITSU, et al.

Application No.: 10/827,371

Filed: April 20, 2004

For: A REPEATER AND AN INTER-NETWORK REPEATING METHOD

CLAIM FOR PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 2003-115568, filed April 21, 2003.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

Date: June 16, 2004

James E. Ledbetter
Registration No. 28,732

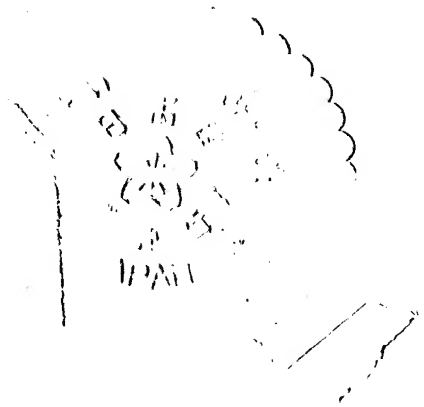
JEL/spp
Attorney Docket No. L8612.04111
STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, NW, Suite 850
P.O. Box 34387
Washington, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　４月２１日
出願番号 Application Number:	特願２００３－１１５５６８
[ST. 10/C]:	[ＪＰ２００３－１１５５６８]
出願人 Applicant(s):	松下電器産業株式会社



２００４年　４月１２日

特許庁長官
Commissioner,
Japan Patent Office　今井康夫

出証番号　出証特２００４－３０３００９４

【書類名】　特許願
【整理番号】　2913050136
【提出日】　平成15年 4月21日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 29/12
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　横光　康志
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　八尾　昭男
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　濱▲崎▼　敏幸
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　小西　宏
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　執行　正浩
【発明者】
【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニックコミュニケーションズ株式会社内
【氏名】　満永　雄二

【発明者】

【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニック
コミュニケーションズ株式会社内

【氏名】　鷲谷　公憲

【発明者】

【住所又は居所】　福岡市博多区美野島４丁目１番６２号　パナソニック
コミュニケーションズ株式会社内

【氏名】　長尾　英明

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　中継装置

【特許請求の範囲】

【請求項１】第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第１ネットワーク側の外部ポート番号が前記第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第２ネットワークに転送する制御手段と、

前記内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、

前記ポートの未使用時間が所定時間になると、前記ポートマッピングテーブルから前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項２】前記未使用時間が、前記第２ネットワークに接続された端末装置からのアクセスにより、ユーザが設定可能であることを特徴とする請求項１記載の中継装置。

【請求項３】前記ポート管理手段が、ポートが開かれている時間をモニタして最長時間を記録し、該最長時間以上の時間を前記未使用時間の閾値として設定することを特徴とする請求項１または２記載の中継装置。

【請求項４】第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第１ネットワーク側の外部ポート番号が前記第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第２ネットワークに

転送する制御手段と、

前記内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、

通信パケットを所定時間受信していないと判断した場合には、前記第２ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合に前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項５】第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第１ネットワーク側の外部ポート番号が前記第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第２ネットワークに転送する制御手段と、

前記第２ネットワーク側に接続された端末装置に存在確認のパケットを定期的に送信するための時間を計時するタイマ手段と、

前記タイマ手段が計時した時刻に前記第２ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合に前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項６】前記ポート管理手段が、前記第２ネットワークに接続された端末からの要求に基づいて前記ポートマッピングテーブルへの登録を行うことを特徴とする請求項１～５のいずれかに記載の中継装置。

【請求項７】中継装置が、ＵＰｎＰ規格に従ってＩＰパケットを動的にポートフォワーディングするルータであることを特徴とする請求項１～６のいずれかに記載の中継装置。

【請求項８】第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第１ネットワーク側の外部ポート番号が前記第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第２ネットワークに転送する制御手段と、

ＤＨＣＰリース期限に再リースをするか否かを確認し、前記端末装置からの再リース要求を受信するＤＨＣＰサーバ部と、

前記端末装置からの再リース要求がなかった場合には、前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ルータなどの中継装置に関し、とくに動的にポートフォワーディング設定を行ってポートを開設するとともに、この動的に開かれたポートを自動的に閉鎖する中継装置に関するものである。

【０００２】

【従来の技術】

インターネット等の広域ネットワークへ常時接続するためＡＤＳＬ，ＣＡＴＶの普及が本格化し、ブロードバンドルータの普及も著しい。しかし、現行のＩＰプロトコルＩＰｖ４ではグローバルＩＰアドレス（以下、外部ＩＰアドレス）の絶対数が不足しているため、ＮＡＴ（Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ）機能やポートフォワーディング機能（静的ＩＰマスカレード）などを使用して外部ＩＰアドレスの不足に対応している。このＮＡＴ機能は、ＬＡＮ側の機器からインターネットへアクセスするときには、そのローカルＩＰアドレス（内部ＩＰアドレス、以下、ＩＰアドレスという）をルータのＷＡＮ側の外部ＩＰアドレスへ変換するものである。

【０００３】

インターネットからＬＡＮ側の特定の機器へアクセスする場合、ルータのポートフォワーディング機能（静的ＩＰマスカレード機能）を用いることでアクセスが可能になる。すなわち、これにはまず予め、ルータにポート番号とＩＰアドレスの変換テーブルを設定しておき、インターネットからアクセスするときには、ルータの外部ＩＰアドレスと外部ポート番号を指定する。このアクセスを受け付けたルータは予め設定された変換テーブルに従い、外部ＩＰアドレスをＩＰアドレスに変換する。この変換によりＩＰアドレスをもったＬＡＮ内の機器にアクセスすることが可能となる。

【０００４】

このポートフォワーディング機能，ＮＡＴ機能により従来のルータは、外部ＩＰアドレスの枯渇を緩和し、ＬＡＮ内の複数のユーザ機器とインターネットとを接続したが、ユーザは機器のポート番号を得て、その設定や変更を手動で行う必要があった。

【０００５】

しかし、手動での設定は煩わしい上に、ポートの活用という点では不十分でもあるため、ＵＰｎＰフォーラムにより、動的にポートフォワーディング設定（ポートマッピング）を行う規格が作成された（非特許文献１参照）。この規格の設定は、配下の端末からルータに対してポートを開設するように要求し、ルータはそれが可能な場合には登録し、使用不可の場合には端末は再度要求し、決定するまでこれを繰り返すものである。なお、ＵＰｎＰ規格ではポートは無期限もしくは有期限で割り当てることができ、この有期限の割り当てを利用すれば、ルータのベンダーによらず動的に設定した外部ポートを自動的に削除させることができる。図１２は従来の動的ポートフォワーディングにおけるポート割当からポート解除までのシーケンスチャートである。

【０００６】

図１２に示すように、外部ＩＰアドレス「２３２．０．０．１」（ＤＨＣＰサーバによって割り当てられたＩＰアドレス「１９２．１６８．０．４」）のルータにＬＡＮ内の内部ポート番号「８０８０」がユーザ設定されたサーバＡを接続すると、サーバＡはＤＨＣＰ発見パケットを送信し、ＤＨＣＰサーバがＩＰアド

レス「１９２．１６８．０．１」を割り当てる。続いてサーバＡはルータ発見パケットを送信し（ｓｑ１０１）、ルータがこれに対して応答する（ｓｑ１０２）。これを受信するとサーバＡはポート登録要求を送信し（ｓｑ１０３）、ルータは外部ポート番号「８０」を割り当てて応答する（ｓｑ１０４）。

【０００７】

その後、インターネットに接続された外部ＩＰアドレス「２３２．０．０．２」のクライアント端末からサーバＡに「ｈｔｔｐ／／：２３２．０．０．１：８０」でアクセスすると（ｓｑ１０５）、ルータは「ｈｔｔｐ／／：１９２．１６８．０．１：８０８０」にポートフォワーディングする（ｓｑ１０６）。サーバＡはこれに対してレスポンスを返し（ｓｑ１０７）、クライアント端末はサーバＡの処理を求めてアクセスし（ｓｑ１０８）、サーバＡはレスポンスを送信する（ｓｑ１０９）。その後、クライアント端末とサーバＡとの間で通信が終了する。その後、ポートの割当てがサーバＡからの無期限の割当要求によるものである場合、通信が終了しているにも関わらず、ポートはサーバＡに割当てられたままとなる。

【０００８】

【非特許文献１】

ＵＰｎＰ規格、［ｏｎｌｉｎｅ］、［平成１５年１月１３日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｕｐｎｐ．ｏｒｇ／ｓｔａｎｄａｒｄｉｚｅｄｄｃｐｓ／ｄｅｆａｕｌｔ．ａｓｐ＞

【０００９】

【発明が解決しようとする課題】

以上説明したように従来のルータのポートフォワーディング機能（静的ＩＰマスカレード機能）は、ＬＡＮ側の端末装置に対して外部ポート番号を用いてアクセスできるものである。しかし、ＬＡＮ側のシステム変更に伴って外部ポート番号に変更が発生した場合、その変更をすべて手動で設定し直さなければならなかった。

【００１０】

また、ＵＰｎＰフォーラムの規格によって動的にポートフォワーディング設定

した場合、ポートの割当てがサーバや端末からの無期限の割当要求によるものである場合、通信が終了しているにも関わらず、ポートはサーバや端末に割当てられたままとなる。従って、サーバの電源がＯＦＦとなった場合や、通信していた端末のアプリケーションが終了した場合には、そのポートが使用されないのにも関わらず、残ったままとなり、このポートがセキュリティホールとなって不正アクセスを許す可能性があった。

【００１１】

そこで本発明は、動的に開かれたポートを設定に従って自動的に閉じる中継装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】

上記の課題を解決するために本発明は、第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、第１ネットワーク側のグローバルＩＰアドレスと外部ポート番号が第２ネットワーク側に接続された端末装置のローカルＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第２ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたものである。

【００１３】

これにより、動的に開かれたポートを設定に従って自動的に閉じることができる。

【００１４】

【発明の実施の形態】

本発明の請求項１は、第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、第１ネットワーク側の外部ポート番号が第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に

関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第２ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、ポートの未使用時間が所定時間を超えたとき、ポート管理手段によってポートを閉鎖するから、ポートが開かれたままでは不正アクセスされる危険があるが、所定時間以上経過するとポートは閉鎖され、これによって端末装置内部の情報が漏れることはない。

【００１５】

本発明の請求項２は、未使用時間が、第２ネットワークに接続された端末装置からのアクセスにより、ユーザが設定可能であることを特徴とする請求項１記載の中継装置であり、ポートを閉鎖するための時間はユーザによってまちまちであるが、ユーザが中継装置にアクセスしてこの時間を任意に設定できるから、手軽に個人個人で最も希望に適ったポート閉鎖を行うことができる。

【００１６】

本発明の請求項３は、ポート管理手段が、ポートが開かれている時間をモニタして最長時間を記録し、該最長時間以上の時間を未使用時間の閾値として設定することを特徴とする請求項１または２記載の中継装置であり、ポートを開いて閉じるまでの時間の利用実態を考慮し、過去の利用の中で最大時間を記憶するので、次の要求に対しては前回利用時間より大きい時間を設定すれば、利用中にも関わらずポートを閉鎖する可能性が低くなり、一方ポートが開いているにもかかわらず利用されていない期間が存在する確率を最小限にすることが可能となる。

【００１７】

本発明の請求項４は、第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、第１ネットワーク側の外部ポート番号が第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パ

ケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第２ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、通信パケットを所定時間受信していないと判断した場合には、第２ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合にポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずにポートが開いたままの状態で終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってカウントアウトするまでポートは使われることなく開いているのを防止できる。

【００１８】

本発明の請求項５は、第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、第１ネットワーク側の外部ポート番号が第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第２ネットワークに転送する制御手段と、第２ネットワーク側に接続された端末装置に存在確認のパケットを定期的に送信するための時間を計時するタイマ手段と、タイマ手段が計時した時刻に第２ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合にポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、一定時間間隔ごとに存在確認パケットを送信して端末の存在を確認するから、アクセスの有無と関係なくポートの使用未使用をチェックすることができ、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了することがなく、ポートが開いたままの状態で終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってカウントアウトするまでポートは使われることなく開いているのを防止できる。

【００１９】

本発明の請求項６は、ポート管理手段が、第２ネットワークに接続された端末

からの要求に基づいてポートマッピングテーブルへの登録を行うことを特徴とする請求項１～５のいずれかに記載の中継装置であり、第２ネットワークに接続したり電源をＯＮしたときに、中継装置の存在を通知するパケットを端末は受信するとポートマッピングの登録が可能であることを知り必要なポートマッピングを中継装置に向けて要求を送信し、これを受信した中継装置のポート管理手段がポートマッピングテーブルへの登録して外部ポート番号を割り当て、ポートを開設できる。

【００２０】

本発明の請求項７は、中継装置が、ＵＰｎＰ規格に従ってＩＰパケットを動的にポートフォワーディングするルータであることを特徴とする請求項１～６のいずれかに記載の中継装置であり、ＵＰｎＰ規格に従ったルータは、無期限だけでなく有期限でポートを割り当てることができるので、ベンダーによらず自動的に第１ネットワーク側の外部ポート番号を設定したり、割り当てを削除することができる。

【００２１】

本発明の請求項８は、第１ネットワークと第２ネットワークとの間の通信パケットの中継を行う中継装置であって、第１ネットワーク側の外部ポート番号が第２ネットワーク側に接続された端末装置の内部ＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第２ネットワークに転送する制御手段と、ＤＨＣＰリース期限に再リースをするか否かを確認し、端末装置からの再リース要求を受信するＤＨＣＰサーバ部と、端末装置からの再リース要求がなかった場合には、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、ＤＨＣＰ機能を利用してきわめて簡単にポートを閉鎖できる。

【００２２】

（実施の形態１）

本発明の実施の形態１における中継装置について説明する。図１は本発明の実

施の形態１における中継装置配下のクライアント端末にアクセスするネットワークシステムの構成図、図２は本発明の実施の形態１における中継装置の構成図、図３は本発明の実施の形態１におけるクライアント端末の構成図、図４は本発明の実施の形態１におけるサーバのの構成図、図５は本発明の実施の形態１におけるポートマッピングテーブルの説明図、図６は本発明の実施の形態１におけるポート割当のフローチャート、図７は本発明の実施の形態１におけるタイマによるポート割当を削除するときのフローチャート、図８は本発明の実施の形態１におけるアクセス後の存在確認によるポート割当を削除するときのフローチャート、図９は本発明の実施の形態１における定期的な存在確認によるポート割当を削除するときのフローチャート、図１０は本発明の実施の形態１におけるポート割当からタイマによるポート削除までのシーケンスの説明図、図１１は本発明の実施の形態１におけるポート割当からアクセス後の存在確認によるポート削除までのシーケンスの説明図である。

【００２３】

図１において、１はＴＣＰ／ＩＰで通信する広域ネットワーク（ＷＡＮ）の１つであるインターネット（本発明の第１ネットワーク）、２はインターネット１と接続可能なインタフェースを有し、ローカルエリアネットワーク（本発明の第２ネットワーク、以下、ＬＡＮという）側のポートを複数備えて配下の各端末装置、例えば後述する画像サーバ３ａ，３ｂ，３ｃに対してルーティングする、とくにＵＰｎＰ規格に従ってＩＰパケットを動的にポートフォワーディングするルータ（本発明の中継装置）、３ａ，３ｂ，３ｃは画像サーバである。４はインターネット１に接続して画像サーバ３ａ，３ｂ，３ｃにアクセスできる端末、５はブラウザ機能を搭載したコンピュータ端末、６はホスト名でアクセスするとグローバルＩＰアドレス（本発明の外部ＩＰアドレス、以下、外部ＩＰアドレスという）を応答するＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバで、７はインターネット１に接続されたウェブサーバある。８は、ＬＡＮ内で所定のローカルＩＰアドレス（本発明の内部ＩＰアドレス、以下、ＩＰアドレスという）の中から画像サーバ３ａ，３ｂ，３ｃにＩＰアドレスを割り当てるＤＨＣＰ（Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サ

ーバである。なお、ＤＨＣＰサーバ８はルータ２に搭載するのでもよい。

【００２４】

実施の形態１においては、画像サーバ３ａ，３ｂ，３ｃをルータ２に接続すると、各サーバはルータ２に外部ポートの割り当てを要求し、使用可能な外部ポート番号を登録する。例えば、実施の形態１の画像サーバ３ａ，３ｂ，３ｃのうちの１台、例えば画像サーバ３ａが外部ポート番号の割り当てを要求したときは、ルータ２は所定の外部ポート番号、例えば「８０」を割り当てる。このとき、インターネット１側からこのポート番号「８０」を有した画像サーバ３ａを認識できることになり、インターネット１側からポート番号「８０」でアクセスしたときは、ルータ２のポートフォワード機能により、画像サーバ３ａ，３ｂ，３ｃのうちの１台である画像サーバ３ａに通信パケットは確実に着信する。なお、ルータ２に登録されるポート番号には、インターネット１側で使用される外部ポート番号と、ＬＡＮ側で使用される内部ポート番号があるが、ＵＰｎＰ規格に従ってルータ２に動的に割り当てようとする外部ポートが既に使用中の場合は別のポート番号を再度割り当てるよう要求を出すことになる。

【００２５】

同様に、他の２つの画像サーバ３ｂ，３ｃに対してルータ２は外部ポートの割り当て例えば「２０００」「２００１」の割り当て要求を行う。これによってインターネット１を介して端末４からユーザがこの外部ポート番号で画像サーバ３ａ，３ｂ，３ｃにアクセスしたとき、画像サーバ３ａ，３ｂ，３ｃへの接続が可能になるものである。

【００２６】

次に、実施の形態１のルータ２の内部構成について図２に基づいて説明する。図２において、１１は画像サーバ３ａ，３ｂ，３ｃのインターネット１との間のグローバルネットワークＩ／Ｆ部、12_1，12_2，・・，12_nはそれぞれ画像サーバ３ａ，３ｂ，３ｃ，・・等に接続されるローカルネットワークＩ／Ｆ部である。複数のグローバルＩＰアドレスを有する場合には、グローバルネットワークＩ／Ｆ部１１は複数設けられる。

【００２７】

１４は制御プログラムや各種データをメモリする記憶部であり、１４ａはポートマッピング情報を割り当てるためのポートマッピングテーブル、１４ｂはポートを閉じるための設定時間を設定するための利用実績メモリ部である。このポートマッピングテーブル１４ａは外部ＩＰアドレスと外部ポート番号をＩＰアドレスと内部ポート番号に関係付けるものである。なお、グローバルネットワークＩ／Ｆ部が一つのときは、外部ＩＰアドレスの関連付けは必ずしも必要ない。

【００２８】

１５は制御部であって、中央演算処理装置（ＣＰＵ）に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。制御部１５は、システム全体の制御を行うとともに、ポートマッピングテーブル１４ａに従ってアドレス変換を行い、受信したパケットをポートフォワーディングする。１６は画像サーバ3.a，３ｂ，３ｃ，・・のポート番号を割り当て、割り当てたポート番号を削除するポート管理手段であり、１７はパケットが通過してからの時間をカウントするタイマ手段である。

【００２９】

実施の形態１のルータ２は、画像サーバ３ａ，３ｂ，３ｃやコンピュータ端末５からの外部ポート番号の無期限の割当て要求により、開いた外部ポートがセキュリティホールとならないように、時間を計る等により開きっぱなしのポートを閉じる。そのための第１の方法は、その外部ポートに対してアクセスがあったときから一定時間またはユーザが設定した時間が経過するとその外部ポートを閉じるもので、タイマ手段１７は時間を計測して閉じるタイミングを検出するものである。第２の方法は、そのポートに対してアクセスがあってから所定の時間を経過すると、通信管理を実行する制御部１５が、その外部ポートへのアクセスのフォワード先に対し、ｐｉｎｇコマンドやＡＲＰコマンドを送信して存在確認を行い、存在しないことが判明した時点にポートを閉じる方法である。第３の方法は、ポート管理手段１６がその外部ポートへのアクセスのフォワード先に対して定期的にｐｉｎｇコマンドやＡＲＰコマンドを送信してＬＡＮ内の端末装置の存在確認を行い、存在しないことが判明した時点にポートを閉じるものである。そして、第４の方法は、ポート割当要求を受信してポートを開き、その後ＤＨＣＰリ

ースの期限が経過したとき再リースの要求がないときポートを閉鎖するものである。詳細は後で説明する。

【００３０】

次に、実施の形態１の画像サーバ３ａ，３ｂ，３ｃの内部構成について図３に基づいて説明する。図３において、２１は画像サーバ３ａ，３ｂ，３ｃのインターネット１との間のネットワークインタフェースであり、端末４のブラウザからのリクエストを画像サーバ３ａ，３ｂ，３ｃに伝え、画像サーバ３ａ，３ｂ，３ｃからのウェブページを表示するためにＨＴＭＬ等のマークアップ言語で記述されたデータやカメラ部２２で撮像した画像をインターネット１に送信する。２２はカメラ部、２３はカメラ部２２に設けられたＣＣＤあるいはＣＭＯＳ撮像素子等からの映像信号であるＲ，Ｇ，Ｂ信号あるいは補色信号を処理し、輝度信号Ｙと色差信号Ｃｒ，Ｃｂ信号を発生してＪＰＥＧ形式、ＭＰＥＧ形式その他の圧縮形式に圧縮する画像データ生成部である。

【００３１】

２４は制御プログラムや各種データをメモリする記憶部であり、２４ａはＨＴＭＬ等のマークアップ言語により表示指示やリンク情報が記述された複数のファイルを記憶しているＨＴＭＬ記憶部、２４ｂは画像データ生成部２３で圧縮した画像データを格納する画像記憶部である。

【００３２】

２５は、プロトコルＴＣＰ／ＩＰでインターネット１との通信を行うウェブサーバ部であり、２６は、端末４のブラウザからウェブサーバ部２５にアクセスがあったときに、ブラウザに対してＨＴＭＬ等で構成されたファイルを記憶部２４から取り出して、状況に応じて動的にＨＴＭＬ等を生成し直し、送信するＨＴＭＬ生成部である。２７は制御部であって、中央演算処理装置（ＣＰＵ）に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。２８はカメラ部２２のパンチルト等の操作を行うモータ等から構成される駆動部、２９は駆動部２８を駆動させるカメラ制御部である。制御部２７は、ブラウザからの要求を処理しＨＴＭＬ生成部２６を動作させてウェブページ用ファイルを生成したり、ブラウザへ送信する画像データを記憶部から取り出したり、さらにカメラ制

御部２９に対してモードを指定して動作させるものである。

【００３３】

続いて、端末４の内部構成について図４に基づいて説明する。３１は端末４のインターネット１との間のネットワークインタフェースであり、画像のリクエストを画像サーバ３ａ，３ｂ，３ｃに伝え、ウェブページを表示するためのＨＴＭＬ等のマークアップ言語で記述されたテキストデータや画像データをインターネット１から受信する。３２はディスプレーに表示を行う表示手段、３３は表示手段３２によって受信したウェブページを表示し、ＧＵＩにより画面上表示した制御ボタンやアイコン等で画像のリクエストを行うブラウザ手段である。

【００３４】

３４は制御プログラムや各種データをメモリする記憶部、３５はキーボードやマウス等の入力手段、３６は音声データを再生することができる音声出力手段である。音声出力手段３６は圧縮されたデータを伸長して再生する。なお、音声出力手段３６はインターネット１を介して受信したプラグインソフトでもよい。３７は制御部であって、中央演算処理装置（ＣＰＵ）に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。

【００３５】

さて、実施の形態１のルータ２において、ＵＰｎＰフォーラムの規格によって動的にポートフォワーディング設定を行うときの動作の説明を図６に基づいて行う。ルータ２は、画像サーバ３ａ，３ｂ，３ｃが接続されたり、電源をＯＮしたり、コンピュータ端末５のアプリケーションが始動したとき、画像サーバ３ａ，３ｂ，３ｃやコンピュータ端末５からポート割当て要求を受信すると、ポート管理手段１６がポートの割当を行い、ポートマッピングテーブル１４ａに登録する。

【００３６】

まず、ルータ２の制御部１５はポート割当要求パケットを受信するまで待機し、ポート割当要求があるか否かをチェックする（ｓｔｅｐ１）。制御部１５は、ポート割当要求がないときは再び待機し、ポート割当要求があった場合にはポート割当が可能か否かがチェックする（ｓｔｅｐ２）。ポート割当が可能である場

合、制御部１５は、ポートを割り当てて応答し（ｓｔｅｐ３）、ポートマッピングテーブル１４ａに登録する（ｓｔｅｐ４）。ｓｔｅｐ２においてポート割当ができない場合には、制御部１５は、ポート割当不可応答を行い（ｓｔｅｐ５）、ｓｔｅｐ１に戻って待機する。

【００３７】

このとき、外部のポート番号とともにポートマッピングテーブル１４ａに登録する内部のポート番号及び内部のＩＰアドレスは、ポート割当要求パケットの中に記載されているが、ポート割当要求のＴＣＰ／ＩＰヘッダ領域から取り込むことも可能である。

【００３８】

ポートマッピングテーブル１４ａには、ＬＡＮ内の内部ポート番号とインターネット１側の外部ポート番号のほかに、画像サーバ３ａ，３ｂ，３ｃのＩＰアドレス、ホスト名、最後のアクセスがあってからポートを閉じるための設定時間が登録される。このＩＰアドレスは、画像サーバ３ａ，３ｂ，３ｃがＤＨＣＰサーバ８に対してＤＨＣＰ発見パケットを送信し、ＤＨＣＰサーバ８が与えたものである。そして、設定時間は画像サーバ３ａ，３ｂ，３ｃの存在確認を行うためにパケットを送信するまでの時間であってもよい。さらに、存在確認を定期的に行うためのｐｉｎｇまたはＡＲＰを送信する時間間隔を登録しておくこともできる。

【００３９】

図５はこのポートマッピングテーブル１４ａの具体例を示している。図５において、ホスト名「マシン１」の画像サーバ３ａは、ＬＡＮに接続されると、ＤＨＣＰサーバ８によってＩＰアドレス「１９２．１６８．０．１」が割り当てられ、ＵＰｎＰ規格のルータ２によって外部ポート番号「８０」が割り当てられる。内部ポート番号「８０８０」は画像サーバ３ａがポートフォワードのためのポート割当要求を行った内部ポート番号である。設定時間１０分はデフォルト値であり、最終のパケットが通過してからポートを閉鎖するまでの時間である。

【００４０】

同様にホスト名「マシン２」に対しては、ルータ２の割り当てた外部ポート番

号「２０００」、内部ポート番号「８０」、ＤＨＣＰサーバ８によって割り当てられたＩＰアドレス「１９２．１６８．０．３」が登録され、設定時間２０分が設定されている。また、ホスト名「マシン３」に対しては、外部ポート番号「２００３」、内部ポート番号「１０１」、ＩＰアドレス「１９２．１６８．０．３」が割り当てられ、設定時間として５分が登録される。このホスト名「マシン２」と「マシン３」の関係は、同一ＩＰアドレスを有しており、例えば、図１のコンピュータ端末５において複数のブラウザアプリケーション（ネットワークエクスプローラ等）を起動させて、起動したブラウザがそれぞれポート割当要求を行ったような場合である。コンピュータ端末５において複数のブラウザアプリケーションを起動させた場合、それぞれのブラウザには、外部との通信のために異なるポート番号が割当てられる（図５においては「８０」，「１０１」）。このように本実施の形態１のルータ２は、設定時間が経過すると画像サーバ３ａ，３ｂ，３ｃやコンピュータ端末５が登録した外部ポートは閉鎖される。

【００４１】

ここで、図７に基づいて画像サーバ３ａ，３ｂ，３ｃがポート割当を受けた後、タイマ手段１７によるポート閉鎖処理について以下説明する。この処理は最終のアクセスがあった後一定時間が経過するとポートを閉じるものである。図７に示すように、ポート割当を行ったポートに対してポート管理手段１６はカウントダウンするための時間をセットする時間フラグを設定する（ｓｔｅｐ１１）。さらにタイマ手段１７により一定時間のカウントを始める。次いでポートフォワードのアクセスがあったか否かがチェックされる（ｓｔｅｐ１２）。ｓｔｅｐ１２において、アクセスがあった場合には該ポートの時間フラグを更新する（ｓｔｅｐ１３）。ｓｔｅｐ１２においてアクセスがない場合、現時刻と時間フラグの時間とを比較し（ｓｔｅｐ１５）、比較した時刻が所定時間を超えているか否かがチェックされ（ｓｔｅｐ１６）、所定時間超えていない場合はｓｔｅｐ１２に戻り、越えた場合はｓｔｅｐ１８に進む。なお、ｓｔｅｐ１３で時間フラグが更新されるのは、ｓｔｅｐ１５，ｓｔｅｐ１６のプロセスを経るため、一定時間が未経過でアクセスがあった場合である。

【００４２】

ｓｔｅｐ１３において、時間フラグを更新した後、ポートフォワードが可能かどうかがチェックされ（ｓｔｅｐ１４）、可能であればパケットをこのポートにフォワーディングして（ｓｔｅｐ１７）、ｓｔｅｐ１２に戻る。ｓｔｅｐ１４でポートフォワードができない場合と、ｓｔｅｐ１６で所定の時間を超えている場合、該当するポートのポート番号をポートマッピングテーブル１４ａから削除する（ｓｔｅｐ１８）。次いで、ルータ２は画像サーバ３ａ，３ｂ，３ｃに対してポート割当強制削除通知を送信して（ｓｔｅｐ１９）、終了する。なお、ｓｔｅｐ１４において、ポートフォワーディングが不可の場合、直ちにｓｔｅｐ１８に進むのではなくて、複数回連続して不可の状態が続いた場合だけ進むようにしてもよい。複数回連続していないときはｓｔｅｐ１２に戻る。

【００４３】

ところで、以上はタイマ手段１７が一定時間をカウントして処理を行ったが、この時間はユーザの利用実態と密接な関係がある。従って、上述したように常に一定時間をカウントするのではなく、ユーザの利用実態に沿った時間を設定してポートを閉鎖するのも好適である。この場合、制御部１５は画像サーバ３ａ，３ｂ，３ｃごと（ユーザごと）の利用実績、すなわちポートを開いてから閉鎖するまでの過去の実績の最大時間を記録しておき、その１１０％の値を閉鎖時間として使用するものである。利用されているかどうか、利用実績の判断はポート開放要求またはパケットの通過実績の有無をモニタすることで行う。ユーザ自身が希望で任意に設定してもよい。

【００４４】

また、上述の説明においては、インターネットから外部ポートへ最終のポートフォワードのアクセスがあった後一定時間が経過するとポートを閉じることとしたが、外部ポートからの最終のポートフォワードのアクセスに加えて、登録された外部ポート番号からインターネットへ送信されていく最後の通信パケットを考慮に入れてポートを閉じることとしてもよい。

【００４５】

このように、本実施の形態１のルータ２は、ＵＰｎＰ規格の動的に開かれたポートを自動的に閉じるためのタイマ手段１７を備えているから、ポート開設され

てから所定時間経過した後ポートを閉じることができる。さらに、ユーザが自分にとって任意の最適時間を設定できるので、もっともユーザにとって好ましい時間を設定できる。また、ポートを開いて閉じるまでの利用実態に沿うように、過去の利用の中で最大時間を記憶するので、次の要求に対しては前回利用時間より大きい時間を設定すれば、利用中にも関わらずポートを閉鎖することはない。

【００４６】

次に、図８に基づいて画像サーバ３ａ，３ｂ，３ｃがポート割当を受けた後、存在確認によって行うポート閉鎖処理について説明する。この処理は画像サーバ３ａ，３ｂ，３ｃがＬＡＮ内に存在しないことが確認されるとポートを閉じるものである。図８に示すように、ポート割当を行ったポートに対してポート管理手段１６は時間フラグを設定する（ｓｔｅｐ２１）。そしてタイマ手段１７は一定時間のカウントを始める。次いでポートフォワードのアクセスがあったか否かがチェックされる（ｓｔｅｐ２２）。ｓｔｅｐ２２において、アクセスがあった場合には時間フラグを更新する（ｓｔｅｐ２３）。ｓｔｅｐ２２においてアクセスがない場合、現時刻と時間フラグの時間とを比較し（ｓｔｅｐ２５）、比較した時刻が所定時間を超えているか否かがチェックされ（ｓｔｅｐ２６）、所定時間超えていない場合はｓｔｅｐ２２に戻り、所定時間が経過している場合は以下説明するｐｉｎｇコマンドやＡＲＰコマンド等の存在確認パケットを送信し（ｓｔｅｐ２８）、応答があるか否かをチェックする（ｓｔｅｐ２９）。なお、ｓｔｅｐ２３で時間フラグが更新されるのは、ｓｔｅｐ２５，ｓｔｅｐ２６のプロセスを経るため、一定時間が未経過でアクセスがあった場合である。

【００４７】

ところで、この存在確認を行うｐｉｎｇコマンドは端末間の通信確認をするためのネットワークコマンドであり、データパケットの送受信が成功したか否かの確認等を行うものである。このコマンドを受信した端末装置はこれを実行することで「ＩＣＭＰメッセージ」を送出する。「ＩＣＭＰメッセージ」を受信することによって通信確認が行え、相手端末の存在も確認できるものである。

【００４８】

また、ＡＲＰ（Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）

は、ＩＰアドレスからＭＡＣアドレスを知るために使われるプロトコルである。ＭＳ－ＤＯＳなどではＡＲＰコマンドを使うことによって、ＭＡＣアドレスを格納しているＡＲＰキャッシュテーブルの設定に問題がないかを確認することができる。ＬＡＮ内にＭＡＣアドレスを知りたいＩＰアドレスを含んだＡＲＰパケットを送信すれば、該当するＩＰアドレスを持つ端末が応答するので、該当マシンのＭＡＣアドレスを知ることができる。ＡＲＰパケットはｐｉｎｇでは応答しない端末（ファイアウォール）を搭載した機器などに対しても有効である。

【００４９】

続いて、ｓｔｅｐ２３において、時間フラグを更新した後、ポートフォワードが可能かどうかがチェックされ（ｓｔｅｐ２４）、可能であればパケットをこのポートにフォワーディングして（ｓｔｅｐ２７）、ｓｔｅｐ２２に戻る。ｓｔｅｐ２４でポートフォワードができない場合と、ｓｔｅｐ２９で応答がなかった場合、該当するポートのポート番号をポートマッピングテーブル１４ａから削除して（ｓｔｅｐ３０）、終了する。ｓｔｅｐ２９で応答があった場合もそのまま終了する。なお、ｓｔｅｐ２４において、ポートフォワーディングが不可の場合、直ちにｓｔｅｐ３０に進むのではなくて、複数回連続して不可の状態が続いた場合だけ進むようにしてもよい。複数回連続していないときはｓｔｅｐ２２に戻る。

【００５０】

次に、図９に基づいて画像サーバ３ａ，３ｂ，３ｃがポート割当を受けた後、ルータ２が定期的に行う存在確認パケットによってポート閉鎖処理について説明する。図９に示すように、タイマ手段１７は定期的にｐｉｎｇまたはＡＲＰを送信する間隔の一定時間をカウントする。所定時間が経過するまでカウントされ、カウントアウトすると（ｓｔｅｐ４１）、ルータ２はｐｉｎｇコマンドやＡＲＰコマンド等の存在確認パケットを送信し（ｓｔｅｐ４２）、応答があるか否かをチェックする（ｓｔｅｐ４３）。

【００５１】

続いて、ｓｔｅｐ４３において応答がなかった場合、該当するポートのポート番号をポートマッピングテーブル１４ａから削除して（ｓｔｅｐ４４）、終了す

る。ｓｔｅｐ４３で応答があった場合もそのまま終了する。

【００５２】

このように一定時間間隔、例えば１０分ごとにｐｉｎｇコマンドやＡＲＰコマンド等の存在確認パケットを送信して端末の存在を確認するから、ネットワークを介してのアクセスの有無と関係なくポートの使用未使用をチェックすることができ、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずポートが開いたまま終了しているような場合にも確実にポートを閉じることができる。上述の２つの方法と異なり、タイマ手段１７がカウントアウトするまではポートが放置されるといったことがない。

【００５３】

続いて、ＬＡＮ内のローカルサーバであるコンピュータ端末５のアプリケーションＡ（例えば、ブラウザアプリケーション）が、インターネット１に接続されたグローバルサーバであるウェブサーバ７にアクセスし、タイマ手段１７によって割当ポートを削除する場合のシーケンスについて説明する。図１０に示すように、コンピュータ端末５が起動すると、ＤＨＣＰ発見パケットを送信してＤＨＣＰサーバ８からの応答を受け取り、ＩＰアドレス「１９２．１６８．０．１」を割り当てられる。ここでコンピュータ端末５はＤＨＣＰサーバ８を使わず、静的に「１９２．１６８．０．１」をユーザが手動で割り付けてもよい。続いてコンピュータ端末５上で起動したアプリケーションＡにはポート番号を「８０８０」がコンピュータ端末５上で割り当てられる。

【００５４】

続いてアプリケーションＡはルータ発見パケットを送信し（ｓｑ１）、ルータ２がこれに対して応答する（ｓｑ２）。これを受信するとアプリケーション５ａはポート登録要求を送信し（ｓｑ３）、ルータ２はポート割当応答を行う。このポート登録要求にはルータ２の外部ポート番号「８０」とアプリケーションＡが使用するポート番号「８０８０」及びＩＰアドレス「１９２．１６８．０．１」が関連付けられており、ルータ２内でも関連付けられた状態で記録される。

【００５５】

インターネット１側の機器から通信開始のパケットを受信するようなアプリケ

ーションＢは、通常サーバアプリケーションであり、例えばウェブサーバなどである。この場合、インターネット上のグルーバルＩＰアドレス「２３２．０．０．２」を持つウェブサーバ７から、ルータ２配下にあるコンピュータ端末５上のアプリケーションＢに接続する際は「ｈｔｔｐ２３２．０．０．１：８０」でアクセスし（ｓｑ５）、ルータ２はこれをフォーワーディングルールに従って「ｈｔｔｐ／／：１９２．１６８．０．１：８０８０」へフォワーディングを行う（ｓｑ６）。フォワーディングされたパケットを受信したアプリケーションＢは、レスポンスパケットをウェブサーバ７へ返す（ｓｑ７）。その後、コンピュータ端末５が事故などでインターネット上から消えた場合、ウェブサーバ７からのアクセスで（ｓｑ８）、要求パケットがコンピュータ端末５へフォワーディング（ｓｑ９）されても、レスポンスパケットは送信されず、これが外部ポート「８０」を使った最後の通信となる。

【００５６】

ルータ２はパケットが登録ポートを通過した時点でタイマ手段１７を毎回更新し、ポートフォワーディングを継続するが、ｓｑ９でパケットが通過した後は更新されることがないため、やがてタイムアウトする。このように所定の時間が経過してもパケットが着信せずタイムアウトした場合、ルータ２はポート割当強制削除通知を画像サーバ３ａに送信し（ｓｑ１０）、ポート番号「８０」をポートマッピングテーブル１４ａから削除する。

【００５７】

同様に、コンピュータ端末５のアプリケーションＢ（例えば、ウェブサーバアプリケーション）へインターネット１に接続されたウェブサーバ７からアクセスがあり、コンピュータ端末５やアプリケーションＢの存在確認によってルータ２が割当ポートを削除する場合のシーケンスについて説明する。以下説明するｓｑ２１～３０は、上述のタイマ手段１７で処理する場合のｓｑ１～ｓｑ１０と基本的に同一である。

【００５８】

コンピュータ端末５が起動すると、ＤＨＣＰ発見パケットを送信してＤＨＣＰサーバ８からの応答を受け取り、ＩＰアドレス「１９２．１６８．０．１」を割

り当てられる。ここでコンピュータ端末５はＤＨＣＰサーバ８を使わず、静的に「１９２．１６８．０．１」をユーザが手動で割り付けてもよい。続いてコンピュータ端末５上で起動したアプリケーション５ａはポート番号を「８０８０」がコンピュータ端末５上で割り当てられる。

【００５９】

続いてアプリケーションＢはルータ発見パケットを送信し（ｓｑ２１）、ルータ２がこれに対して応答する（ｓｑ２２）。これを受信するとアプリケーションＢはポート登録要求を送信し（ｓｑ２３）、ルータ２はポート割当応答を行う（ｓｑ２４）。このポート登録要求にはルータ２の外部ポート番号「８０」とアプリケーションＢが使用するポート番号「８０８０」及びＩＰアドレス「１９２．１６８．０．１」が関連付けられており、ルータ２内でも関連づけられた状態で記録される。

【００６０】

その後、インターネット上のグルーバルＩＰアドレス「２３２．０．０．２」を持つウェブサーバ７から、ルータ配下にあるコンピュータ端末５上のアプリケーションＢに接続する際は「ｈｔｔｐ２３２．０．０．１：８０」でアクセスし（ｓｑ２５）、ルータ２はこれをフォーワーディングルールに従って「ｈｔｔｐ／／：１９２．１６８．０．１：８０８０」へフォワーディングを行う（ｓｑ２６）。フォワーディングされたパケットを受信したアプリケーションＢは、レスポンスパケットをウェブサーバ７へ返す（ｓｑ２７）。その後、コンピュータ端末５が電源断などでインターネット上から消えた場合、ウェブサーバ７からのアクセスで（ｓｑ２８）、要求パケットがコンピュータ端末５へフォワーディング（ｓｑ２９）されても、レスポンスパケットは送信されず、これが外部ポート「８０」を使った最後の通信となる。

【００６１】

ｓｑ２９でレスポンスのパケットが通過すると、ルータ２はタイマ手段１７により所定の時間が経過するまでカウントする。この時間内に次のパケットが着信すればルータ２はポートを更新し、ポートフォワーディングを続けるが、所定の時間が経過してもパケットが着信しなかった場合、ルータ２はアプリケーション

ＢまたはコンピュータＡ端末５の存在確認を行う（ｓｑ３０）。

【００６２】

存在確認パケットに対して応答がなければ、外部ポート番号「８０」と関連する事項をポートマッピングテーブル１４ａから削除し、存在確認パケットに対して応答があった場合、ルータ２はポート割当強制削除通知を画像サーバ３ａに送信し（ｓｑ１１）、外部ポート番号「８０」と関連する事項をポートマッピングテーブル１４ａから削除する。

【００６３】

ｐｉｎｇコマンドやＡＲＰコマンド等の存在確認パケットを送信してアプリケーションＢまたはコンピュータＡ端末５の存在を確認するから、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずにポートが開いたままの状態で終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってタイムアウトするまでポートは使われることなく開いているのを防止できる。

【００６４】

最後に、図示はしないが、ポート割当要求を受信してポートを開き、その後ＤＨＣＰに対する再リースの要求がないとき、ポートを閉鎖する場合について説明する。従って、ルータ２がＤＨＣＰサーバ機能を備えているのが望ましい。

【００６５】

この実施の形態の場合、ルータ２はＤＨＣＰサーバ８の代わりにＤＨＣＰサーバ部（図示しない）を搭載し、ＬＡＮ内の画像サーバ３ａ，３ｂ，３ｃやコンピュータＡ端末５等の端末のＩＰアドレスの割当を行うとともに、ＤＨＣＰ機能を利用し、これらの端末がＬＡＮ内に不存在であることを、ＤＨＣＰリースの期限切れに行われる端末からの再リース要求の有無で確認する。これによってポートを閉じるものである。

【００６６】

ＤＨＣＰのプロトコルによればリース期限の設定が可能であるが、このときリース期限終了前に再リースをするか否かを確認することが規定されている。この実施の形態はこの規定を利用するもので、一旦ポート割当要求してポートが開か

れた端末が、ＤＨＣＰリースの期限が切れてもＩＰアドレスの更新をしないということがその端末がＬＡＮ内に存在しなくなったことを意味する、と判断するものである。

【００６７】

このため、ルータ２のＤＨＣＰサーバ部は、ＤＨＣＰリース期限が到来すると、再リースするかをこの端末に確認し、再リース要求がされない場合には、ポート管理手段１６がポートマッピングテーブル１４ａを検索し、そのポート番号を削除することによりポートを閉鎖する。この場合、ルータ２のＤＨＣＰ機能を利用し、きわめて簡単にポートを閉鎖できる。

【００６８】

【発明の効果】

本発明の中継装置によれば、ポートの未使用時間が所定時間を超えたとき、ポート管理手段によってポートを閉鎖するから、ポートが開かれたままでは不正アクセスされる危険があるが、所定時間以上経過するとポートは閉鎖され、これによって端末装置内部の情報が漏れることはない。

【００６９】

定期的に存在確認パケットを送信して端末の存在を確認するから、アクセスの有無と関係なくポートの使用未使用をチェックすることができ、正常に終了することがなく、ポートが開いたままの状態で終了している場合等にも確実にポートを閉じることができる。中継装置のＤＨＣＰ機能を利用すればきわめて簡単にポートを閉鎖できる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における中継装置配下のクライアント端末にアクセスするネットワークシステムの構成図

【図２】

本発明の実施の形態１における中継装置の構成図

【図３】

本発明の実施の形態１におけるクライアント端末の構成図

【図４】

本発明の実施の形態１におけるサーバのの構成図

【図５】

本発明の実施の形態１におけるポートマッピングテーブルの説明図

【図６】

本発明の実施の形態１におけるポート割当のフローチャート

【図７】

本発明の実施の形態１におけるタイマによるポート割当を削除するときのフローチャート

【図８】

本発明の実施の形態１におけるアクセス後の存在確認によるポート割当を削除するときのフローチャート

【図９】

本発明の実施の形態１における定期的な存在確認によるポート割当を削除するときのフローチャート

【図１０】

本発明の実施の形態１におけるポート割当からタイマによるポート削除までのシーケンスの説明図

【図１１】

本発明の実施の形態１におけるポート割当からアクセス後の存在確認によるポート削除までのシーケンスの説明図

【図１２】

従来の動的ポートフォワーディングにおけるポート割当からポート解除までのシーケンスチャート

【符号の説明】

１　インターネット

２　ルータ

３ａ，３ｂ，３ｃ　画像サーバ

４　端末

５　コンピュータ端末

６　ＤＮＳサーバ

７　ウェブサーバ

８　ＤＨＣＰサーバ

１１　グローバルネットワークＩ／Ｆ部

12_1，12_2，・・，12_n　ローカルネットワークＩ／Ｆ部

１４　記憶部

１４ａ　ポートマッピングテーブル

１４ｂ　利用実績メモリ部

１５　制御部

１６　ポート管理手段

１７　タイマ手段

２１　ネットワークインタフェース

２２　カメラ部

２３　画像データ生成部

２４　記憶部

２４ａ　ＨＴＭＬ記憶部

２４ｂ　画像記憶部

２５　ウェブサーバ部

２６　ＨＴＭＬ生成部

２７　制御部

２８　駆動部

２９　カメラ制御部

３１　ネットワークインタフェース

３２　表示手段

３３　ブラウザ手段

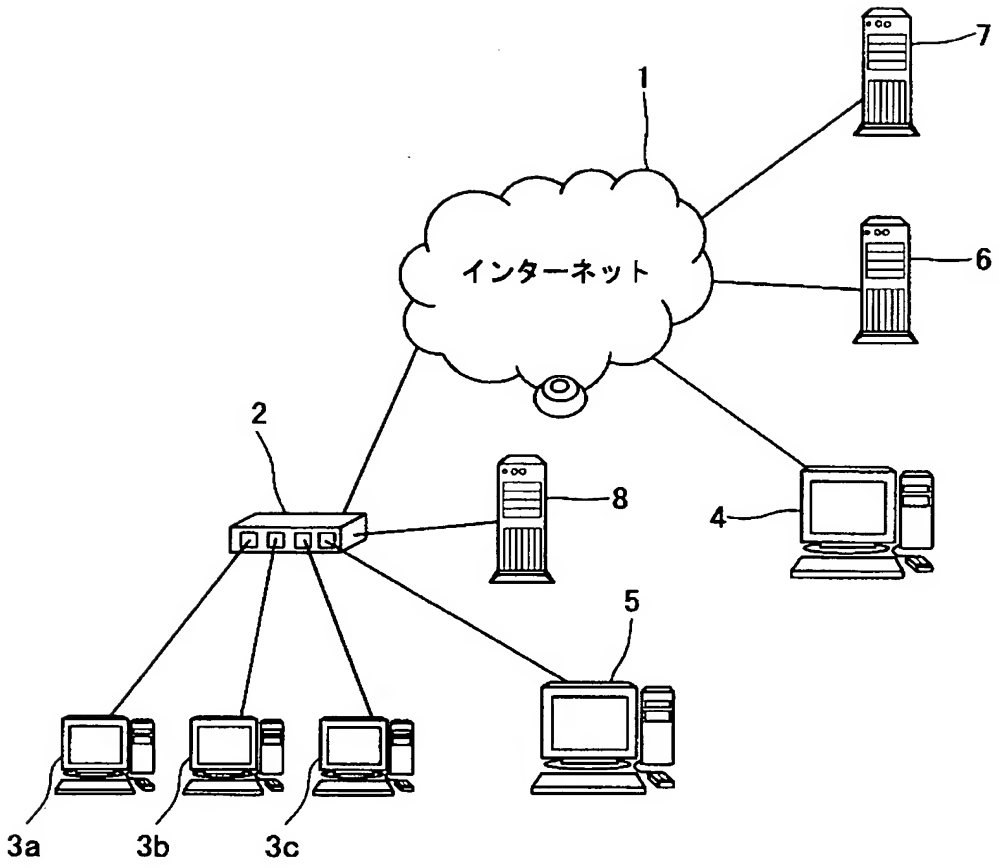
３４　記憶部

３５　入力手段

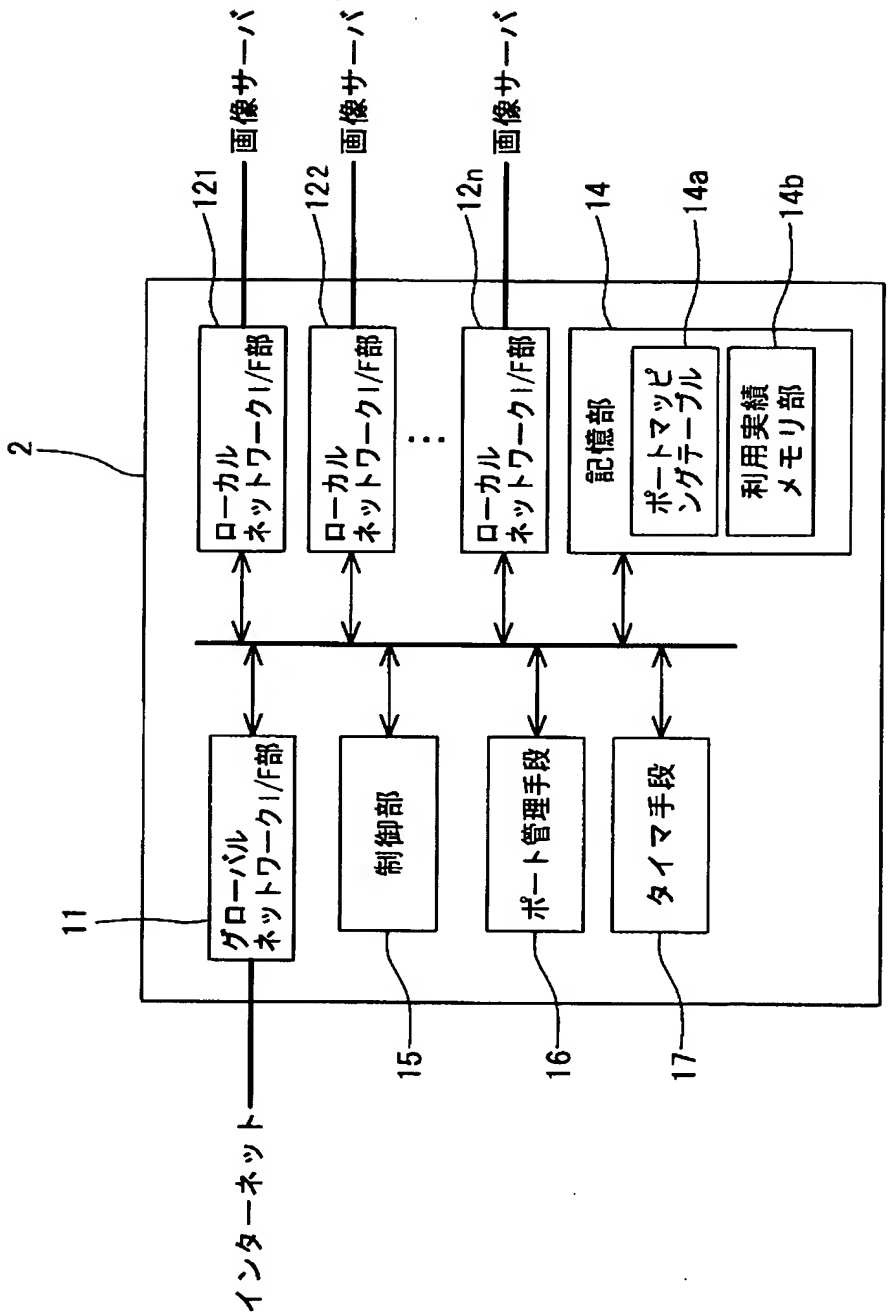
３６　音声出力手段

【書類名】　図面

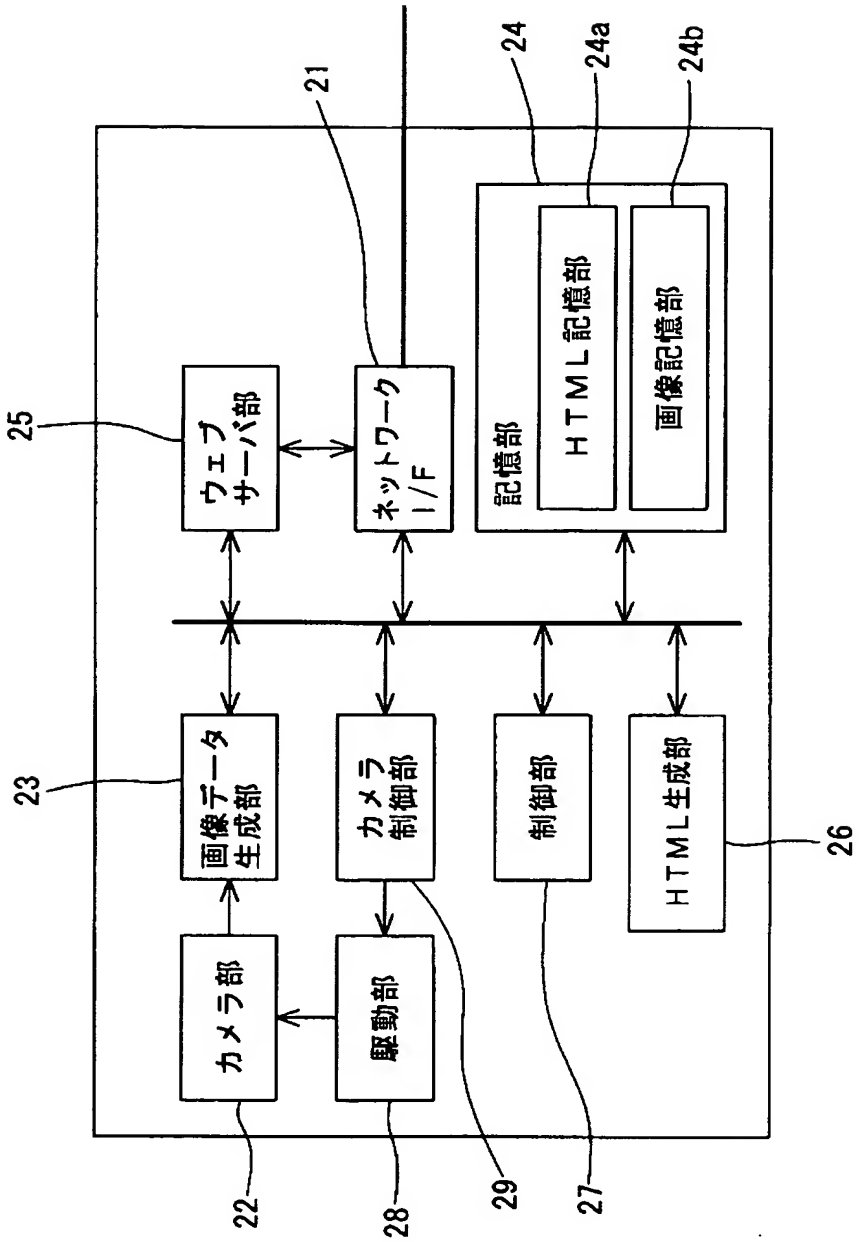
【図１】



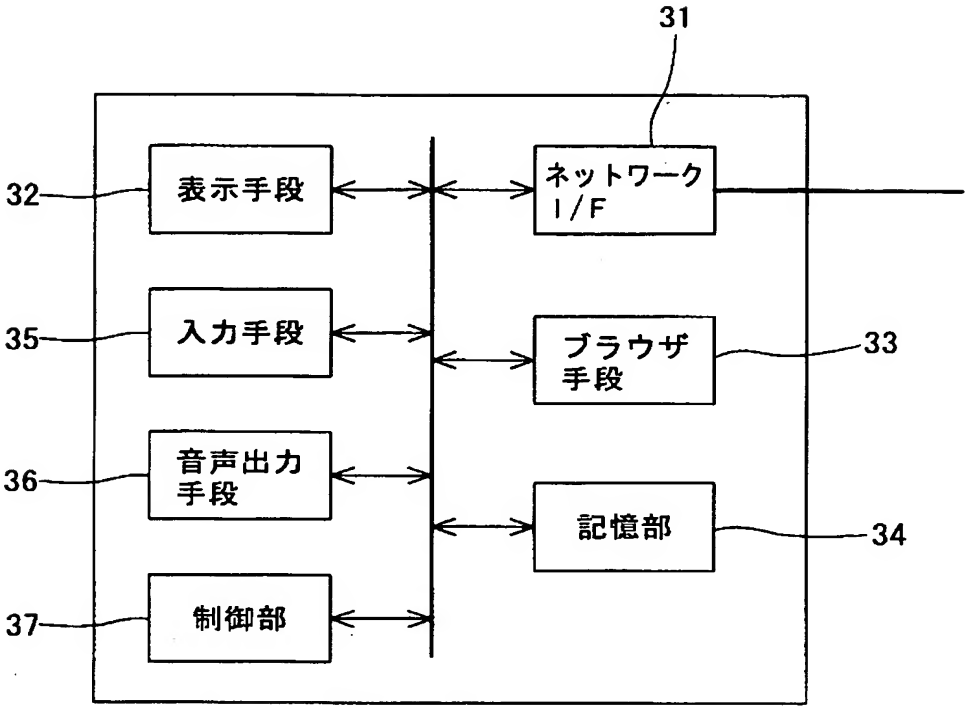
【図２】


画像サーバ
画像サーバ
画像サーバ
121
122
12n
14
14a
14b
2
ローカルネットワークI/F部
ローカルネットワークI/F部
ローカルネットワークI/F部
記憶部
ポートマッピングテーブル
利用実績メモリ部
グローバルネットワークI/F部
制御部
ポート管理手段
タイマ手段
11
15
16
17
インターネット

【図３】


21
24
24a
24b
25
ウェブサーバ部
ネットワークI/F
記憶部
HTML記憶部
画像記憶部
23
画像データ生成部
カメラ制御部
制御部
HTML生成部
26
カメラ部
駆動部
22
28
29
27

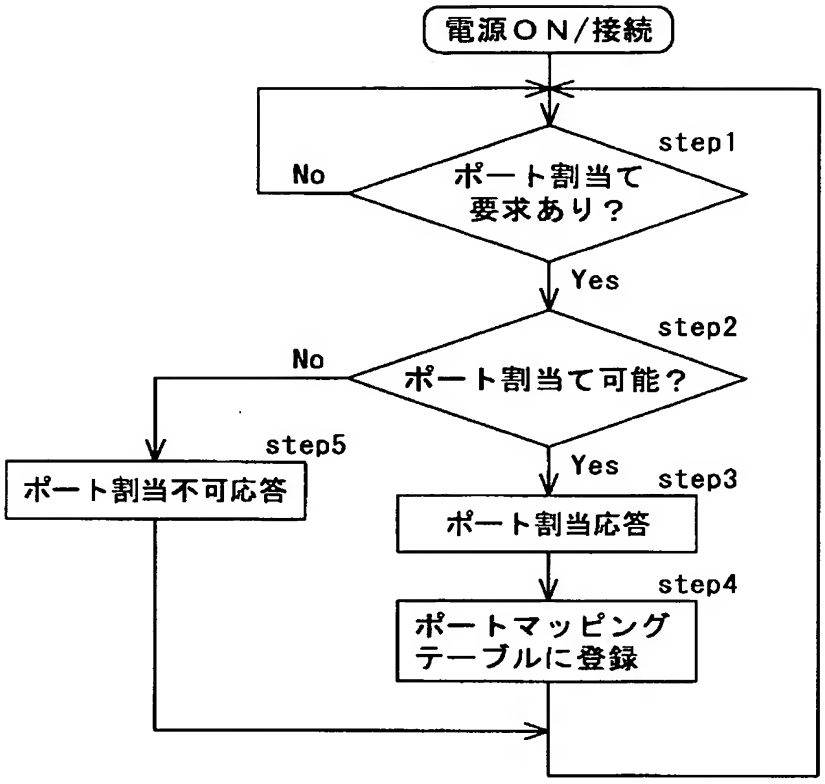
【図４】



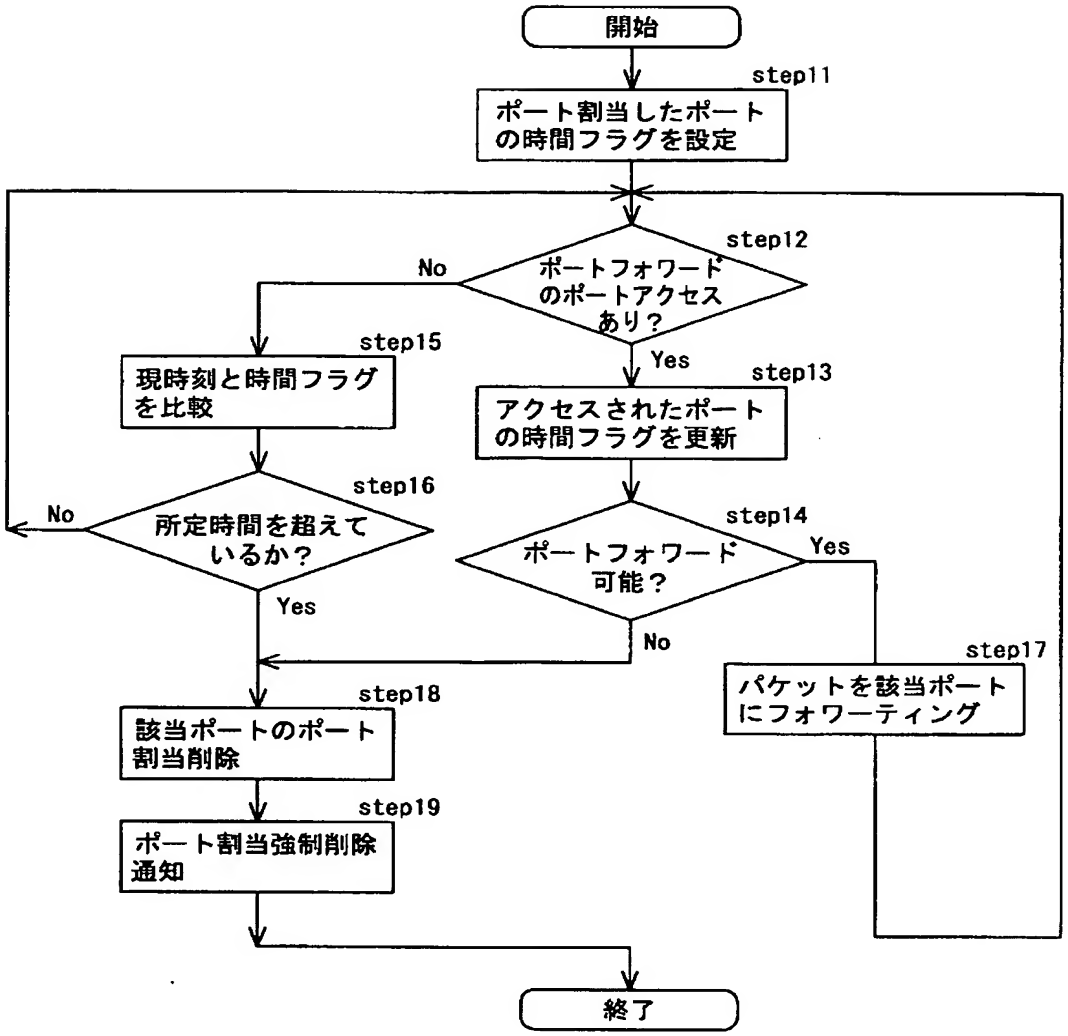
【図５】

ルータ外側		ルータ内側			
外部ﾎﾟｰﾄ番号	外部IPｱﾄﾞﾚｽ	内部ﾎﾟｰﾄ番号	ＩＰアドレス	ホスト名	設定時間
80	232.0.0.2	8080	192.168.0.1	マシン1	（１０分）
2000		80	192.168.0.3	マシン2	２０分
2003		101	192.168.0.3	マシン3	５分

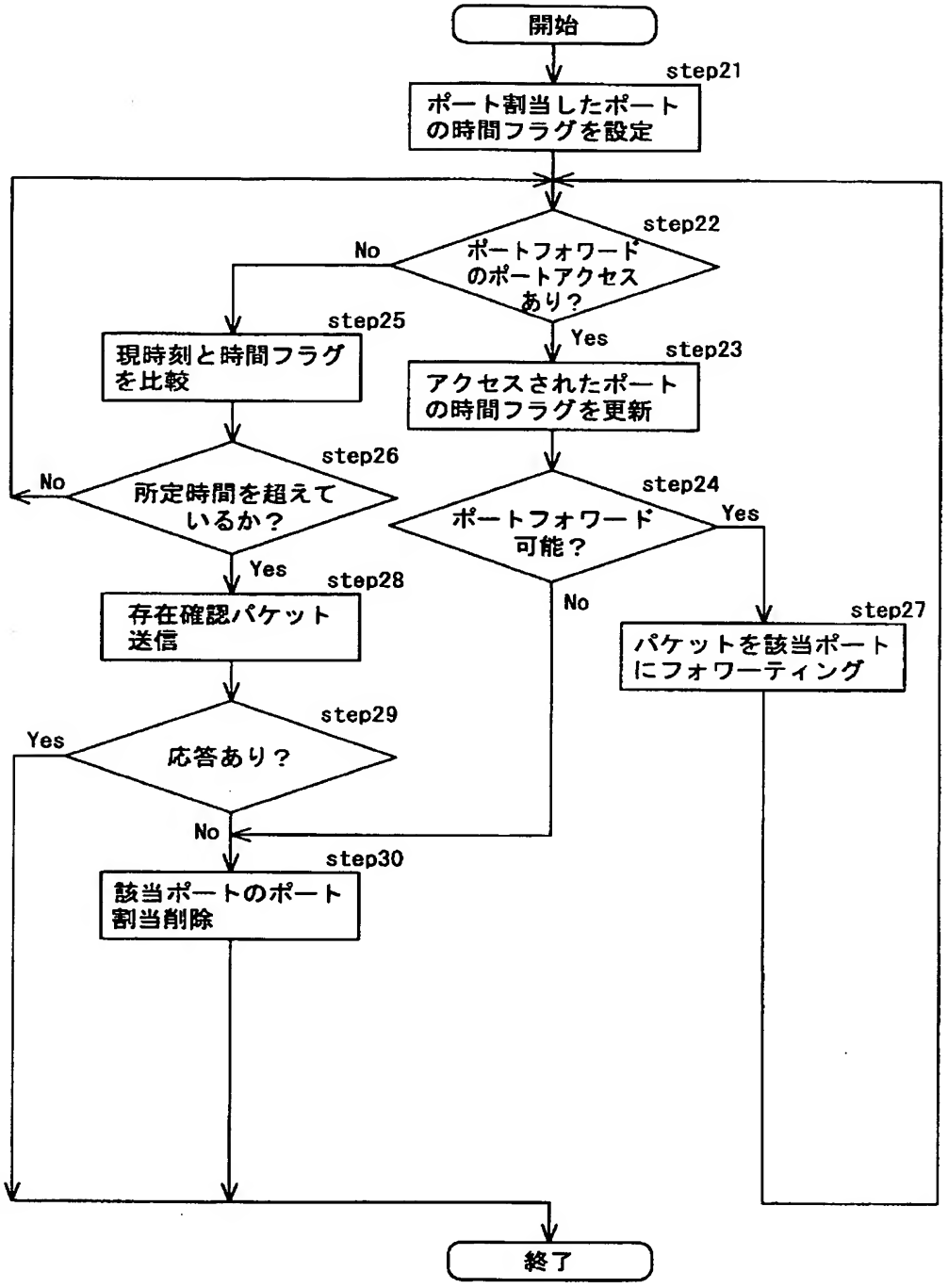
【図６】


電源ＯＮ/接続
step1
No
ポート割当て
要求あり？
Yes
step2
No
ポート割当て可能？
step5
ポート割当不可応答
Yes
step3
ポート割当応答
step4
ポートマッピング
テーブルに登録

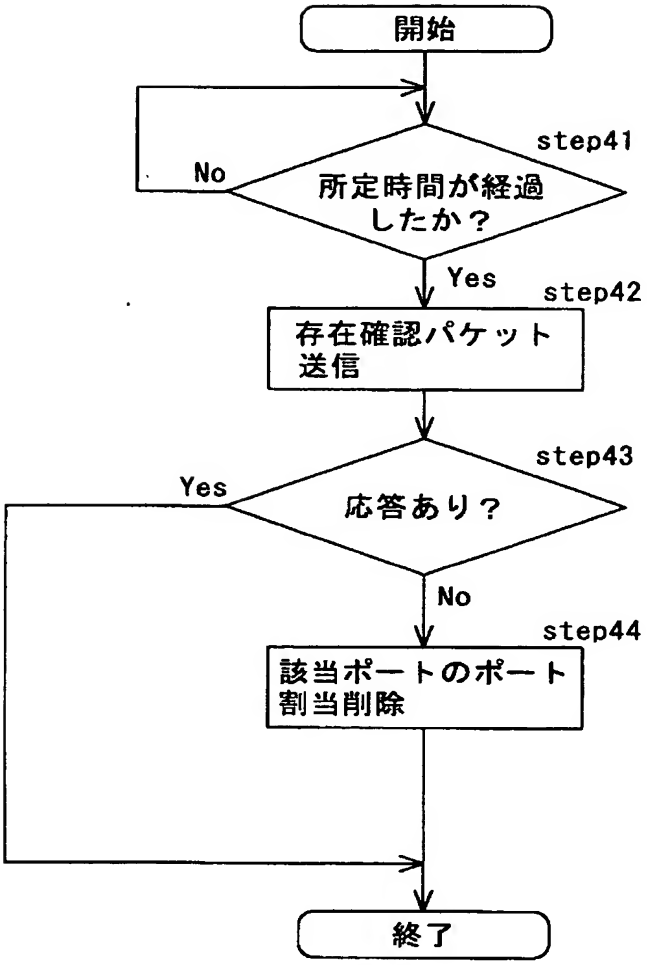
【図７】


開始
step11
ポート割当したポートの時間フラグを設定
step12
ポートフォワードのポートアクセスあり？
No
Yes
step15
現時刻と時間フラグを比較
step13
アクセスされたポートの時間フラグを更新
step16
所定時間を超えているか？
No
Yes
step14
ポートフォワード可能？
Yes
No
step17
パケットを該当ポートにフォワーティング
step18
該当ポートのポート割当削除
step19
ポート割当強制削除通知
終了

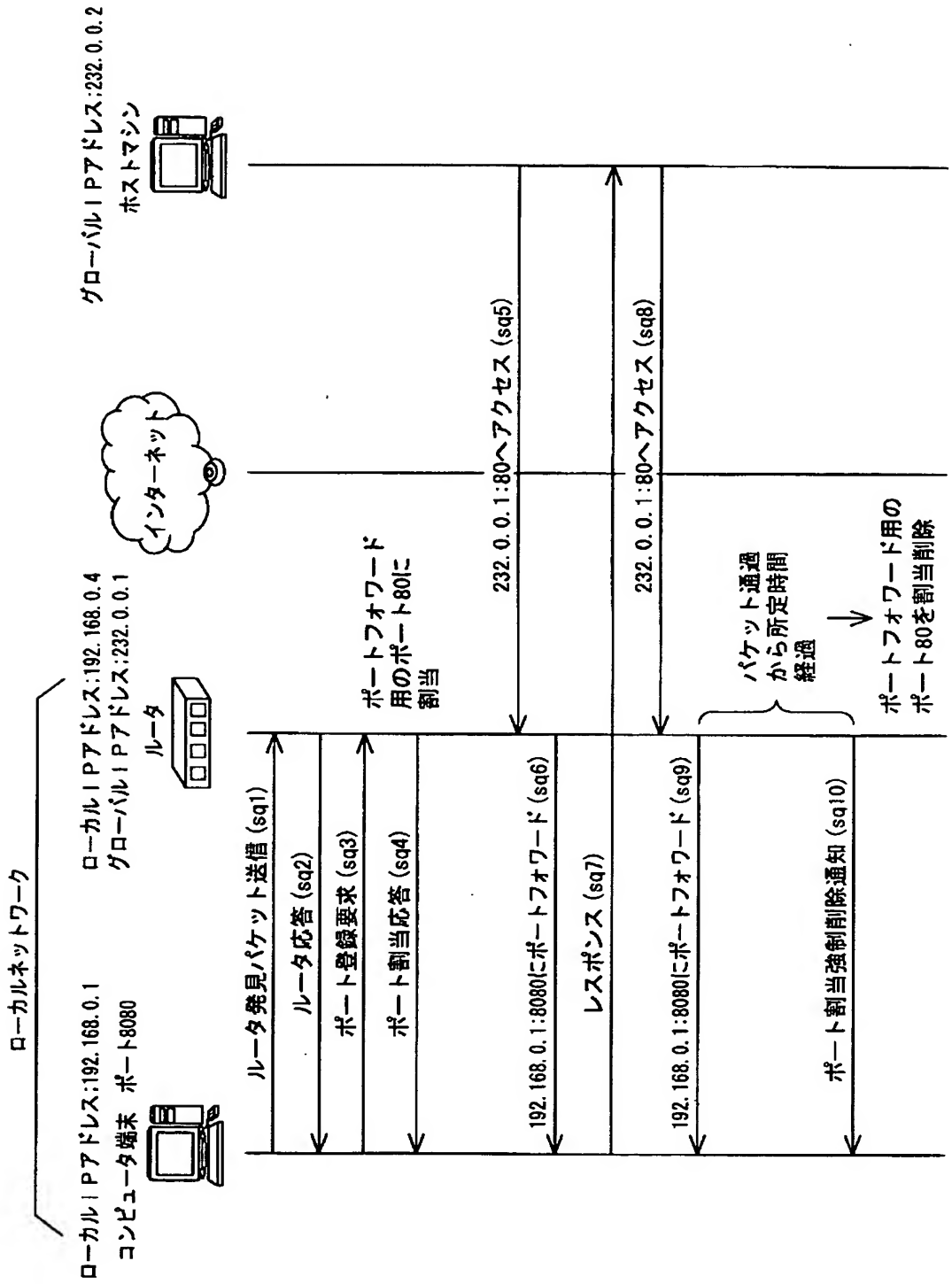
【図８】


開始
step21
ポート割当したポート
の時間フラグを設定
step22
ポートフォワード
のポートアクセス
あり？
No
Yes
step25
現時刻と時間フラグ
を比較
step23
アクセスされたポート
の時間フラグを更新
step26
所定時間を超えて
いるか？
No
Yes
step24
ポートフォワード
可能？
Yes
No
step28
存在確認パケット
送信
step27
パケットを該当ポート
にフォワーティング
step29
応答あり？
Yes
No
step30
該当ポートのポート
割当削除
終了

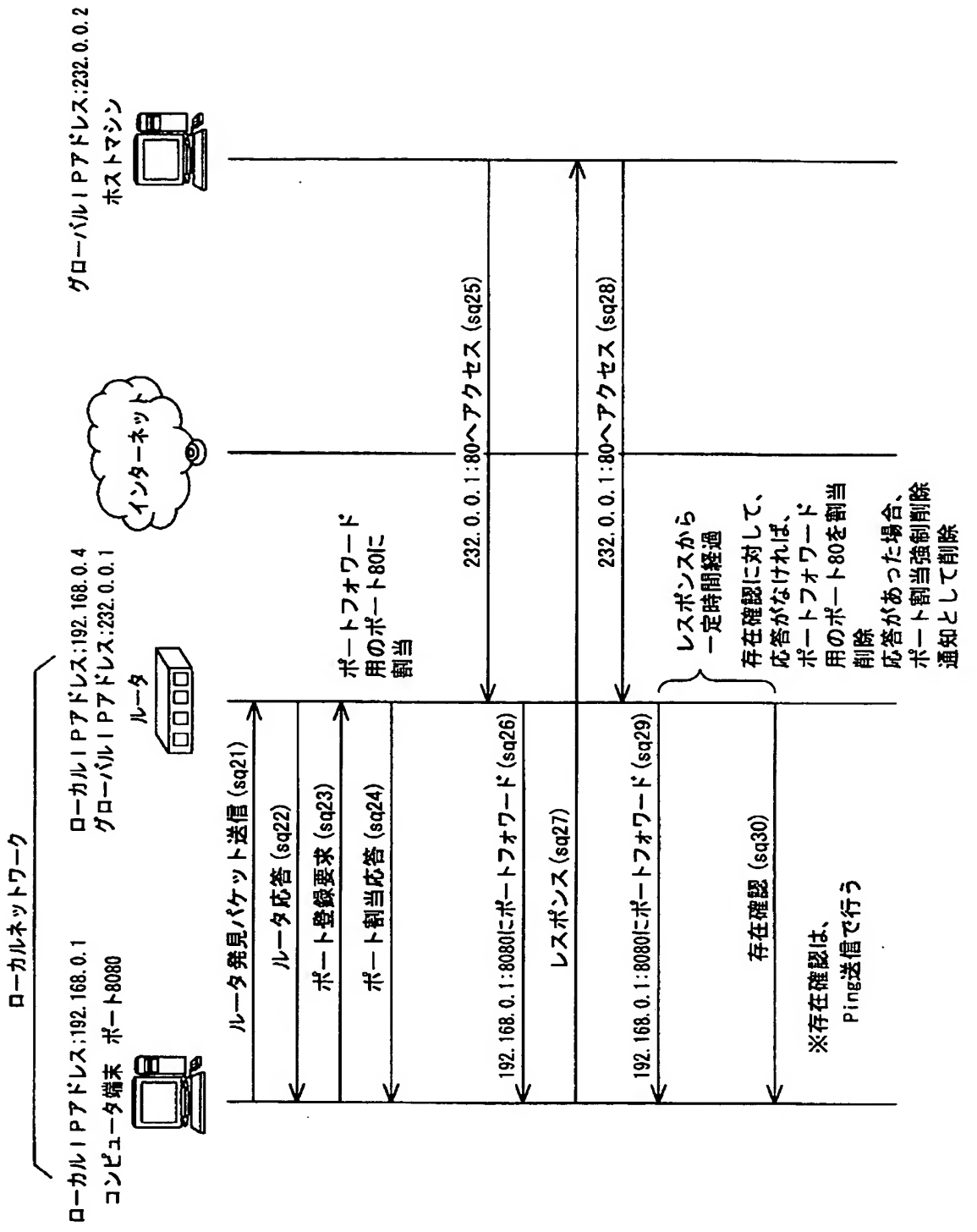
【図９】


開始
step41
No
所定時間が経過したか？
Yes
step42
存在確認パケット送信
step43
Yes
応答あり？
No
step44
該当ポートのポート割当削除
終了

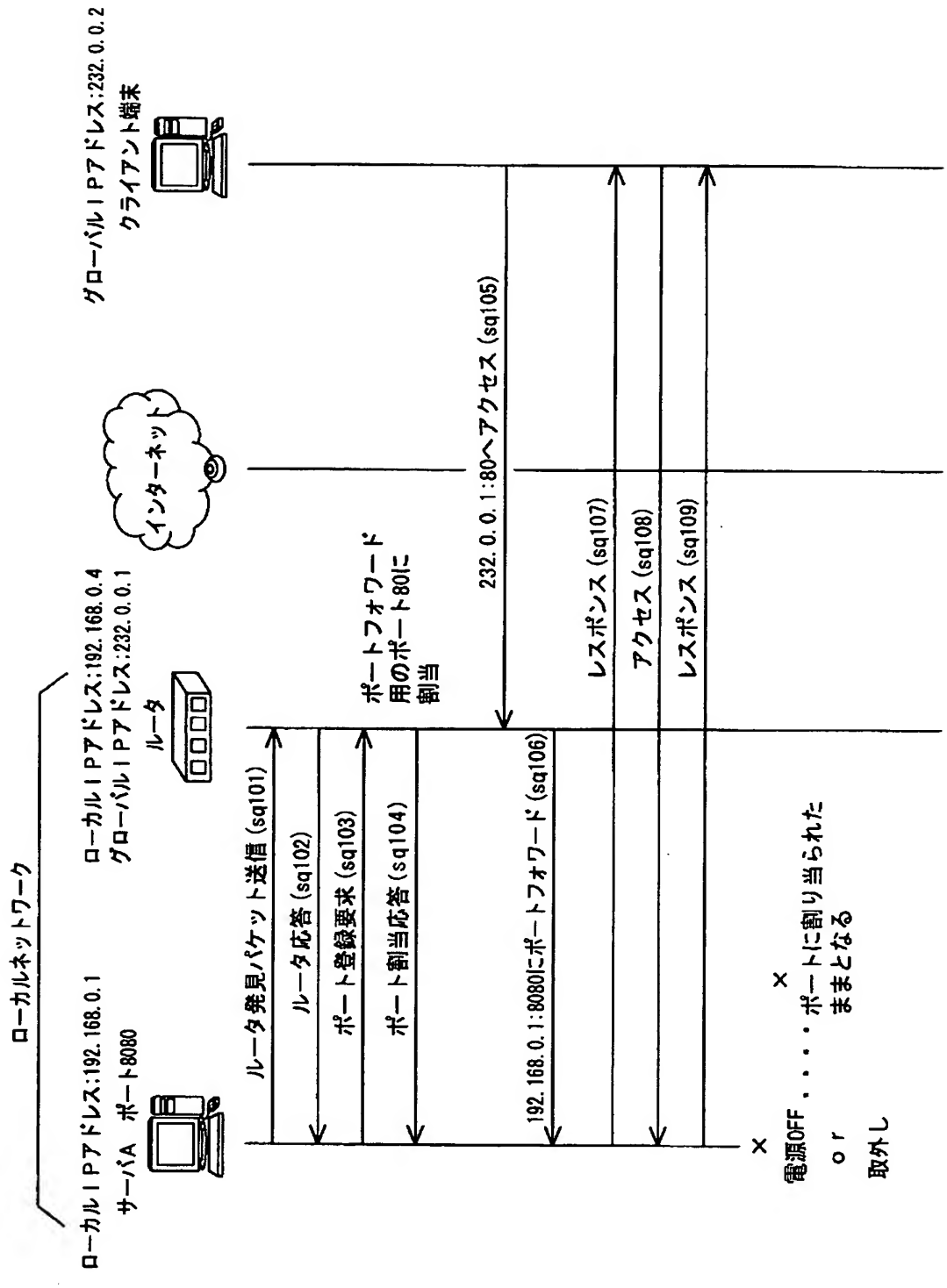
【図１０】


ローカルネットワーク
ローカルIPアドレス:192.168.0.1
コンピュータ端末　ポート8080
ローカルIPアドレス:192.168.0.4
グローバルIPアドレス:232.0.0.1
ルータ
インターネット
グローバルIPアドレス:232.0.0.2
ホストマシン
ルータ発見パケット送信 (sq1)
ルータ応答 (sq2)
ポート登録要求 (sq3)
ポート割当応答 (sq4)
ポートフォワード用のポート80に割当
232.0.0.1:80へアクセス (sq5)
192.168.0.1:8080にポートフォワード (sq6)
レスポンス (sq7)
232.0.0.1:80へアクセス (sq8)
192.168.0.1:8080にポートフォワード (sq9)
パケット通過から所定時間経過
ポートフォワード用のポート80を割当削除
ポート割当強制削除通知 (sq10)

【図１１】


ローカルネットワーク
ローカルIPアドレス:192.168.0.1
コンピュータ端末　ポート8080
ローカルIPアドレス:192.168.0.4
グローバルIPアドレス:232.0.0.1
ルータ
インターネット
グローバルIPアドレス:232.0.0.2
ホストマシン
ルータ発見パケット送信 (sq21)
ルータ応答 (sq22)
ポート登録要求 (sq23)
ポート割当応答 (sq24)
ポートフォワード用のポート80に割当
232.0.0.1:80へアクセス (sq25)
192.168.0.1:8080にポートフォワード (sq26)
レスポンス (sq27)
232.0.0.1:80へアクセス (sq28)
192.168.0.1:8080にポートフォワード (sq29)
存在確認 (sq30)
※存在確認は、Ping送信で行う
レスポンスから一定時間経過
存在確認に対して、応答がなければ、ポートフォワード用のポート80を割当削除
応答があった場合、ポート割当強制削除通知として削除

【図１２】


ローカルネットワーク
ローカルIPアドレス:192.168.0.1
サーバA ポート8080
ローカルIPアドレス:192.168.0.4
グローバルIPアドレス:232.0.0.1
ルータ
インターネット
グローバルIPアドレス:232.0.0.2
クライアント端末
ルータ発見パケット送信 (sq101)
ルータ応答 (sq102)
ポート登録要求 (sq103)
ポート割当応答 (sq104)
ポートフォワード用のポート80に割当
232.0.0.1:80へアクセス (sq105)
192.168.0.1:8080にポートフォワード (sq106)
レスポンス (sq107)
アクセス (sq108)
レスポンス (sq109)
×
電源OFF・・・・ポートに割り当られたままとなる
or
取外し

【書類名】　要約書

【要約】

【課題】　本発明は、動的に開かれたポートを設定に従って自動的に閉じる中継装置を提供することを目的とする。

【解決手段】　本発明は、インターネット側のグローバルＩＰアドレス及び外部ポート番号、または外部ポート番号がＬＡＮ側に接続された端末装置のローカルＩＰアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換してＬＡＮに転送する制御手段と、外部ポート番号を指定した通信パケットを転送してから該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると登録マシンがＬＡＮ上に存在するかどうかを確認して存在していない場合は、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたものである。

【選択図】　図１

特願２００３－１１５５６８

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社